Privacy Risk Assessment for Online Government Applications and Websites Why is it Needed?

In enacting this act, the Legislature recognizes two constitutional rights:

> *the public's right of access to information concerning the conduct of the public's business;*
> *the right of privacy in relation to personal data gathered by governmental entities.*

The Legislature also recognizes a public policy interest in allowing a government to restrict access to certain records, as specified in this chapter, for the public good.

Government Records Access and Management Act
63-2-102 Utah Code

It's All About Gaining and Keeping the Public's Trust

If an effective privacy policy and its helper good security practices are not implemented, the alternatives have been identified as the "show-stoppers" for electronic commerce in the private world. Theft of your credit card numbers, fraud, violence, exploitation of minors and even stealing your identity are becoming more prevalent as vast information stores go online. There is no reason for us to believe that the public sector is immune from these problems.

In this environment, it's all about gaining and keeping the public's trust that we will be good data stewards. Our e-government efforts will be judged in part by how good we are at communicating to the public about how the personal data they disclose to us will be used. In fact, with some of the public at least, government has a continuing uphill battle to fight to establish public trust. This is understandable since government can, and sometimes does, exert powerful influence over our lives. Government can come to our aid in times of crisis, or it can be seen as a barrier to achieving even the simplest of our objectives.

What is a Privacy Risk Assessment and How Can it Help?
As we mentioned it's all about trust. This assessment is one simple tool among others that can get people to use the application you just built. The greater the percentage of customer traffic you can re-direct to the Web, the more efficient your agency can become in serving your customers.

So, what does a privacy risk assessment tool do?

- It can give you a quick snapshot of what your potential risks to the privacy of citizens who use your web application.
- It can very quickly help you to identify whether or not your applications are collecting personally identifiable information.
- It can then assist you in categorizing your level of risk as low, medium, or high.
- Since security decisions have cost impacts, different levels of risk will require different levels of security. This can assist you when you need to talk with your information technology security administrator about what procedures need to be put in place with your application.
- If you can answer the questions in this tool, you will have much of the information you need to communicate to the users of your website about how their personally identifiable information is used and who gets to see it.

What is a Practical Example of How the Tool Can Help?

You have been asked to make it simpler for people with driver's licenses to change their address online. Before you do this, the tool will guide you through a set of questions. For example, it would be helpful to know which laws govern the use of the information you plan to collect online. Are different fields in your application protected under different classifications and laws? Are different pieces of information you collect have different levels of risk if security and privacy are compromised? If you discover that any information that you collect online is private should you check to see if the information is encrypted between the citizen's browser and your server? However, if the personally identifiable information collected is available to anyone because it is in the public interest to do so, does it make sense to spend money on a secure connection? Are certain types of information identified as high risk and so it raises the question about whether certain fields of information should be encrypted at the database level? The tool doesn't answer these questions for you but it gives you a beginning set of questions that can serve as a guide to your planning as you move forward with designing and building your application. Your security administrator can assist you with answering which security tools are right for you after you have completed the privacy risk assessment.

Privacy Risk Assessment
8/15/01

1) Does this application or website collect **personally identifiable information? If yes, proceed to question 2. If no, the assessment is concluded.** Some examples of personally identifiable information include:
   a) First and last name,
   b) Physical address,
   c) E-mail address,
   d) Telephone number,
   e) Social Security number,
   f) Credit card information,
   g) Bank account information, and
   h) Any combination of data that could be used to determine identity.

2) Do any federal statutes, regulations or state statutes other than Government Records Access Management Act (GRAMA), control access to any of this data? If so, what statute(s) or regulations (e.g. HIPAA)? (Guidance: It is important here if you are governed by several laws to create a matrix or checklist to identify which data elements are covered by which laws and identify for each and how access is restricted, if at all.)

3) Is personally identifiable information collected by this application classified under GRAMA? If so, is it private, protected, controlled or public? (Guidance: Using a matrix or checklist would be useful here.)
   a) If so, how are each of the specific data elements in the application classified?
   b) If a data element (or sets of data) are classified as public does the public interest outweigh the need to make this information private?
   c) If a data element (or sets of data) are classified as private does the public interest outweigh the need to *keep* this information private?
   d) If the data is classified as private, what other entities have access to the data? (Guidance: In this case an “entity” may be governmental or non-governmental i.e. an insurance company may have access to a personal driving history record.)

4) Given the information collected, what is the greatest risk associated with an unauthorized entity having access to this information? Please indicate in a-g whether the risk is HIGH, MEDIUM, or LOW for each.
   a) identity theft – name, address, birth date, social security numbers;
   b) impersonation of a professional or entity licensed or registered by a government agency;
   c) theft of financial information like credit card numbers;
   d) release of medical and health information/DNA to employers, prospective employers or insurers;
   e) release of personally identifiable information that enables others to locate an individual for the purpose of perpetrating a crime against that individual such as stalking, rape, domestic violence, other assaults, or sexual abuse and exploitation of minors;
   f) malicious alteration of information in government databases;
   g) Other, please specify

5) What security procedures have been put into place to reduce the risks identified in Question 4? (Guidance: e.g., Secure Socket Layer (SSL) connection between client browser and

server; database encryption, other security measures.

6) Is a link to the state privacy policy statement and any additional agency privacy information which describes how this data is used and is this statement conspicuously displayed on, or linked to from, the agency website?

7) Is the public told in the agency privacy policy located on the website, who has access to their information under a federal statute, federal regulation, a state law other than GRAMA or the status and classification of this information under the Government Records Access and Management Act?

8) Is each data field of information requested through this application absolutely necessary for the agency to conduct this service? Guidance: Risk is lower if the agency does not collect any more information than is needed to accomplish the task.